Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1–27 (CANCELED)

28 (PREVIOUSLY PRESENTED). A network based web content identification and control system for wide area networks, like the Internet, comprising:

client computer(s), which are any computers in the network;

an examiner host computer, which is a remote third-party host computer in the wide area network, being outside of the local network sphere of:

(a) the client computers,

(b) any intermediate computer intercepting client requested web content,

(c) and, any source host computer of the client requested web content;

wherein the examiner host is an independently operating host as a master server, rather than a subordinate slave server such as a database server;

wherein the examiner host controls its processes and resources independently, rather than under direct external command;

performing an on-demand remote identity check on a specially established tiny-sized independent identification of the web content, what is used as a preferred method of processing rather than processing said web content as such;

wherein said identification is a data object which is based on certain property(ies) of said web content so that a unique representation of the identity of said web content is established in smaller size;

wherein said identity check relies on said identification in preference over obtaining said web content itself to said identity check;

wherein said identity check is performed by the examiner host in response to a remote service request;

wherein said identification is delivered without said web content for said identity check, in response to a client direct request to receive said web content from the network;

wherein in response to said identity check service request, the examiner host reserves to the service requestor a temporary service-specific:

(a) service access,
(b) service communication bridge,
(c) and, service process;

wherein the examiner host returns the results of said identity check as a feedback, and on the basis of said results:

(a) it is performed safety or preventive measures,
(b) and / or, it is informed said client,
(c) or, no specific actions are performed;

wherein the web content comprises file(s), web page(s), e-mail message(s), e-mail message attachment(s) or any data which a client can acquire from the network.

29 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 28, comprising:

wherein said identity check comprises the examiner host comparing the delivered identification to stored identifications of web content.

Claim 30 (CANCELED)

31 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 29, comprising:

wherein said delivered identification consists of file identification information and / or data identification information;

wherein a said stored identification consists of file identification information and / or data identification information;

wherein said file identification information comprises one or more of the following properties of the web content:

(a) source URL-address or other type of address,
(b) source computer URL-address or other type of address,
(c) name,
(d) type,
(e) content type,
(f) size,
(g) creation date,
(h) version number,
(i) publisher,
(j) authentication certificate,
(k) or, other properties;

wherein said data identification information comprises:

(a) a check-sum or any identification value based upon the data of the web content,
(b) and / or, a data sample picked according to a certain pattern, algorithm or other rule from the web content.

Claim 32 (CANCELED)

33 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 29, comprising:

wherein said stored identifications belong to known virus infected web content.

34 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 33, comprising:

wherein said safety measures include one or more of the following:

(a) preventing the download of the examined web content to the client computer,

(b) performing a virus scan on the examined web content in the client computer or in the examiner host computer,

(c) destroying the examined web content.

35 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 34, comprising:

wherein the examiner host calculates an estimate for the security threat level of the examined web content and informs it to the client.

36 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 33, comprising:

intermediate computer(s), which are any computers in the network capable to intercept data which client computers receive from the network;

wherein said delivered identification is delivered to the examiner host computer by a said intermediate computer.

37 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 36, comprising:

wherein said safety measures include one or more of the following:

(a) the intermediate computer preventing the download of the examined web content to the client computer,

(b) the intermediate computer performing a virus scan on the examined web content,

(c) the intermediate computer destroying the examined web content.

38 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 36, comprising:

wherein a said intermediate computer is:

(a) a server of the local area network,

(b) a server of the internet service provider,

(c) or, a network node computer.

39 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 29, comprising:

wherein said stored identifications belong to known non-wanted web content.

40 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 39, comprising:

wherein said preventive measures include preventing the download of the examined web content to the client computer, and / or destroying the examined web content.

41 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 39, comprising:

intermediate computer(s), which are any computers in the network capable to intercept data which client computers receive from the network;

wherein said delivered identification is delivered to the examiner host computer by a said intermediate computer.

42 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 41, comprising:

wherein said preventive measures include the intermediate computer preventing the download of the examined web content to the client computer, and / or the intermediate computer destroying the examined web content.

43 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 41, comprising:

wherein a said intermediate computer is:

(a) a server of the local area network,

(b) a server of the internet service provider,

(c) or, a network node computer.

44 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 28, comprising:

wherein said client computers are host computers into which data is uploaded.

Claims 45 –46 (CANCELED)

47 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 29, comprising:

wherein said safety or preventive measures are performed when said comparison yields a confirmed match.

48 (PREVIOUSLY PRESENTED). A network based web content identification and control system according to claim 47, comprising:

wherein if said comparison does not yield a definite match, then a close enough resemblance of the delivered identification to any of the stored identification(s) is deemed to be a confirmed match.

49 (PREVIOUSLY PRESENTED). A network based web content identification and control system for wide area networks, like the Internet, comprising:

client computer(s), which are any computers in the network;

an examiner host computer, which is a remote third-party host computer in the wide area network, being outside of the local network sphere of:

(a) the client computers,

(b) any intermediate computer intercepting client requested web content,

(c) and, any source host computer of the client requested web content;

wherein the examiner host is an independently operating host as a master server, rather than a subordinate slave server such as a database server;

wherein the examiner host controls its processes and resources independently, rather than under direct external command;

a client creating an ad-hoc independent identification for a web content by selectively extracting data item(s) from said web content or by generating data signature(s) on the basis of selected data of said web content;

the client delivering said identification without said web content to the examiner host which performs in response to the client service request an on-demand analysis for said identification;

wherein said analysis relies on said identification in preference over obtaining said web content itself to said analysis;

wherein in response to said client made service request, the examiner host reserves to the client a temporary service-specific:

(a) service access,
(b) service communication bridge,
(c) and, service process;

on the basis of said analysis, the examiner host determining whether the web content to which said identification belongs is:

(a) a security threat or not,
(b) or, non-wanted or not;

the examiner host returning feedback to the client on the basis of said analysis;

wherein the web content comprises file(s), web page(s), e-mail message(s), e-mail message attachment(s) or any data which a client can acquire from the network.

50 (PREVIOUSLY PRESENTED). A network based web access control method for wide area networks, like the Internet, comprising:

a client preparing to access a web-address to receive web content from the network;

the client creating an ad-hoc independent identification which contains at least:

(a) said web-address,

(b) or, a part of said web-address which identifies the pertinent host;

the client delivering said identification to an examiner host which performs in response to the client service request an on-demand identity check for said identification;

wherein the examiner host is a remote third-party host computer in the wide area network, being outside of the local network sphere of:

(a) the client computer,

(b) any intermediate computer intercepting client requested web content,

(c) and, any source host computer of the client requested web content;

wherein the examiner host is an independently operating host as a master server, rather than a subordinate slave server such as a database server;

wherein the examiner host controls its processes and resources independently, rather than under direct external command;

wherein said identity check relies on said identification in preference over obtaining said web content itself to said identity check;

wherein in response to said client made service request, the examiner host reserves to the client a temporary service-specific:

(a) service access,

(b) service communication bridge,

(c) and, service process;

on the basis of said identity check, the examiner host determining whether the entity to which said identification belongs is:

(a) a security threat or not,

(b) or, non-wanted or not;

the examiner host providing feedback to the client on the basis of said identity check;

wherein said web-address is a URL-address or other type of address.

51 (PREVIOUSLY PRESENTED). A network based web access control method according to claim 50, comprising:

preventing client access to the web content under said web-address if the examiner host determines said entity to be a security threat or non-wanted.

52 (PREVIOUSLY PRESENTED). A network based web access control method according to claim 50, comprising:

an intermediate computer creating and delivering said identification on behalf of the client, and receiving feedback from the examiner host on behalf of the client;

wherein the intermediate computer is any computer in the network capable to intercept data which the client receives from the network.

53 (PREVIOUSLY PRESENTED). A network based web access control method according to claim 52, comprising:

the intermediate computer:

(a) informing the client,

(b) and / or, preventing client access to the web content under said web-address,

if the examiner host determines said entity to be a security threat or non-wanted.

Claim 54 (CANCELED).

55 (PREVIOUSLY PRESENTED). An independent host computer which examines identifications of web content, for wide area networks, like the Internet, comprising:

an examiner host which is a remote third-party host computer in the wide area network;

wherein the examiner host examines on demand in real-time tiny-sized independent identifications of web content outside of the local network spheres of the dissemination source, dissemination route and dissemination target of the web content;

wherein a said identification is provided and delivered to the examiner host without the pertinent web content by a client which is either in the dissemination source, dissemination route or dissemination target of said web content;

wherein the examination of said identification is performed in response to the client service request;

wherein said identification is a data object which is based on certain property(ies) of said web content so that a unique representation of the identity of said web content is established in smaller size;

wherein said examination relies on said identification in preference over obtaining said web content itself to said examination;

wherein the examiner host is an independently operating host as a master server, rather than a subordinate slave server such as a database server;

wherein the examiner host controls its processes and resources independently, rather than under direct external command;

wherein in response to said client made service request, the examiner host reserves to the client a temporary service-specific:

(a) service access,
(b) service communication bridge,
(c) and, service process;

wherein on the basis of said examination, the examiner host determines whether the web content to which said identification belongs is:

(a) a security threat or not,
(b) or, non-wanted or not;

wherein the examiner host returns feedback to the client on the basis of said examination;

wherein the web content comprises file(s), web page(s), e-mail message(s), e-mail message attachment(s) or any data which can be acquired from the network.